

REMARKS

Favorable consideration of this Response and Request for Reconsideration, in light of the following discussion, is respectfully requested.

Claims 1-10 and 15-53 are pending in the present Application. Claims 1-5, 9, 10 and 15-52 have been withdrawn from consideration. No new matter has been added.

By way of summary, the Official Action presents the following issues: Claims 6-8 and 53 stand rejected under 35 U.S.C. § 102 as being anticipated by Tatebayashi et al. (U.S. Patent No. 6,028,937, hereinafter Tatebayashi).

REJECTION UNDER 35 U.S.C. § 102

The Official Action has rejected Claims 6-8 and 53 under 35 U.S.C. § 102 as being anticipated by Tatebayashi. The Official Action states that Tatebayashi discloses all of the Applicants' claim limitations. Applicants respectfully traverse the rejection.

Amended Claim 6 recites, *inter alia*, an information processing apparatus, including:

receiving means for receiving a key category from said another information processing apparatus;

selection means for selecting the processing for reciprocal authentication being executed from one or more reciprocal authentication procedures in keeping with said pre-set processing; . . .

key creation means for establishing a common key shared with said another processing apparatus based on the key category.

By way of background, copy protection systems are provided to preclude the copying of original content. In order to combat illegal copying, there must exist a mutual authentication from content servers and portable devices. However, if such authentication is based on hardware, hardware must be replaced to update the authentication algorithm.

Likewise, if the authentication is software-based, the software may be analyzed and modified to circumvent the protection.¹

In light of at least the above deficiency in the art, the present invention is provided. With this object in mind, a brief comparison of the claimed invention, in view of the cited references, is believed to be in order.

FAILURE TO PRESENT A PRIMA FACIE CASE OF ANTICIPATION

Applicants submit that the Official Action of July 26, 2005 has failed to present a *prima facie* case of anticipation with respect to Claim 6-8 and 53 under 35 U.S.C. § 102.

Tatebayashi describes a system in which authentication is performed between a supplier device and a user device. The supplier device (170) and the user device (190) communicate via a network (185).² As shown more specifically in Fig. 5, Tatebayashi describes a simple method of authenticating a communication between two devices. Specifically, a random number generator (71) of the supplier device generates a random number (R1) and transmits it as challenge data (CHA1) to the user device. Upon obtaining the first random number, the user device obtains a second random number (R2) from its own first random number generator (94). The user device then links the first random number and the second random number and encrypts this data with an authentication key (KS) stored in an authentication key storage unit (92) of the user device. This message, which then includes the first random number, the second random number, and an authentication key (KS) is provided to the supplier device as challenge data (RESCHA).³

¹ Application at pages 1-2.

² Tatebayashi at Fig. 3; column 9, lines 15-17.

³ Tatebayashi at col. 9, lines 15-47.

A. Tatebayashi does not disclose or suggest a receiving unit which receives a key category from another information processing apparatus.

As can be appreciated from the description above, the random numbers R1 and R2 are exchanged between the supplier and user device for the purposes of authenticating these devices. R1 is delivered to the user device as challenge data (CHA1). At the second device, a key (KS) is appended to the first random number, and a second random number of the second device is added. This challenge data (RESCHA) is then decrypted and returned to the supplier device. Note that regardless of the value of R1, KS is returned in message RESCHA. Accordingly, neither R1, nor R2, are used to identify a key category as presently recited in the Applicants' claims.⁴

Conversely, Applicants invention is directed toward a reciprocal authentication processing in which a common key is shared between two devices in accordance with a key source category. As shown more specifically in Figs. 38 and 39 of Applicants' specification, a portable device (6) negotiates with a second device via a reciprocal authentication processing in which random number, device identification and a key category number (G) is utilized to generate a transient key (Kab).⁵ Note, at step 423 of Fig. 38, the Key number J of master Key Kna is found from the key category number. In this manner, a more secure authentication processing is configured to prevent unauthorized copying. Tatebayashi does not disclose or suggest reciprocal authentication including receiving a key category number from another information processing apparatus or generating a common key in accordance with the key category number.

⁴ The Official Action asserts, at page 3, that random number challenge data anticipates the Applicants' "key category."

⁵ Application at pages 108-110.

It is well established that each word of every claim must be given weight. *See In Re Wilson*, 424 F.2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970). Further, it is well established that while the U.S. Patent and Trademark Office is to give claim language its broadest “reasonable” interpretation, this does not mean that the U.S. Patent and Trademark Office can completely ignore the understanding that the artisan would have of the term “category” obtained in light of the specification so as to ascribe a completely different and unknown meaning to the term “category” (*See In Re Cortright*, 165 F.3d 1353, 1358, 49 U.S.P.Q. 2d 1464, 1467 (Fed. Cir. 1999)’ (“Although the PTO must give claims their broadest reasonable interpretation, this interpretation must be consistent with the one those skilled in the art would reach.”) and *In Re Okuzawa*, 537 F.2d 545, 548, 190 U.S.P.Q. 464, 466 (C.C.P.A. 1976) citing *In Re Royka*, 490 F.2d 981, 984, 180 U.S.P.Q. 580, 582-83 (C.C.P.A. 1974) (“Claims are not to be read in a vacuum, and while it is true they are given the broadest *reasonable* interpretation during prosecution, their terms still have to be given the meaning called for by the specification of which they form a part.”).

As can be appreciated, Applicants’ key category enables a selection function within a device to select from among one or more reciprocal authentication procedures based on a key category. Likewise, a key is created based upon the key category. Tatebayashi discloses no such structure or methodology.

Accordingly, Applicants respectfully request that the rejection of Claims 6-8 and 53 under 35 U.S.C. § 102 be withdrawn.

CONCLUSION

Should the Examiner continue to disagree with the above distinctions, Applicants respectfully request that the Examiner provide an explanation via Advisory Action pursuant to MPEP § 714.13 specifically rebutting the points raised herein for purposes of facilitating the appeal process.

Please note in accordance with the discussion herein, should the rejections in the Official Action of July 26, 2005 be maintained, Applicants intend to request a Pre-Brief Appeal Conference in accordance with the pilot program outlined in the Official Gazette Notice of July 12, 2005.

Consequently, in view of the foregoing amendment and remarks, it is respectfully submitted that the present Application, including Claims 6-8 and 53, is patently distinguished over the prior art, in condition for allowance, and such action is respectfully requested at an early date.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Scott A. McKeown
Registration No. 42,866

BDL:SAM:ycs

I:\ATTY\SAM\PROSECUTION WORK\204478\RESP DUE 26OCT05.DOC